

SUBSCRIBER AUTHENTICATION IN A MOBILE COMMUNICATIONS SYSTEM

Patent number: JP11513853 (T)

Publication date: 1999-11-24

Inventor(s):

Applicant(s):

Classification:

- international: H04L9/32; H04W12/06; H04L9/32; H04W12/00; (IPC1-7): H04L9/32; H04Q7/38

- european: H04L9/32A; H04Q7/38A; H04W12/06

Application number: JP19960515546T 19961016

Priority number(s): WO1996FI00543 19961016; US19950544199 19951017

Abstract not available for JP 11513853 (T)

Abstract of correspondent: **WO 9715161 (A1)**

[Translate this text](#)

An authentication in a GSM based mobile communications system relies on a challenge and response principle. A 32-bit Signed Response (SRES) parameter is calculated by A3 algorithm from a 128-bit Random Number (RAND) and a 128-bit Authentication Key Ki in a mobile station and in an authentication center, and the SRES values are compared. A CAVE algorithm having a 152-bit input parameter and an 18-bit output parameter is employed as the A3 algorithm. Parameter adaptation functions are provided between the input parameter of the CAVE algorithm and the GSM type input parameters, namely the random number RAND and the authentication key Ki, as well as between the output parameter of the CAVE algorithm and the GSM output parameter, namely the signed response SRES.

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平11-513853

(43) 公表日 平成11年(1999)11月24日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 A

審査請求 未請求 予備審査請求 有 (全 30 頁)

(21) 出願番号 特願平9-515546
(86) (22) 出願日 平成8年(1996)10月16日
(85) 翻訳文提出日 平成10年(1998)4月15日
(86) 国際出願番号 P C T / F I 9 6 / 0 0 5 4 3
(87) 国際公開番号 W O 9 7 / 1 5 1 6 1
(87) 国際公開日 平成9年(1997)4月24日
(31) 優先権主張番号 0 8 / 5 4 4 , 1 9 9
(32) 優先日 1995年10月17日
(33) 優先権主張国 米国 (U S)

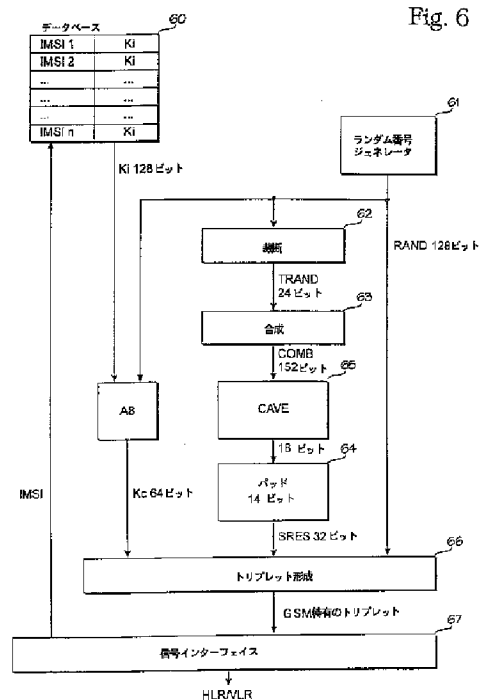
(71) 出願人 ノキア テレコミュニケーションズ オサケ
ユキチュア
フィンランド エフイーエン-02150 エ
スプー ケイララーデンティエ 4
(72) 発明者 ムルト ユハーニ
アメリカ合衆国 テキサス州 75019 コ
ッペル スワロウ ドライブ 758
(74) 代理人 弁理士 中村 稔 (外6名)

最終頁に続く

(54) 【発明の名称】 移動通信システムにおける加入者確認

(57) 【要約】

G S Mベースの移動通信システムにおける確認は、チャレンジ・アンド・レスポンスの原理に基づいている。移動ステーション及び確認センターにおいて128ビットのランダム番号 (R A N D) 及び128ビットの確認キー (K i) からA3アルゴリズムにより32ビットの符号応答 (S R E S) パラメータが計算され、そしてS R E S値が比較される。152ビットの入力パラメータ及び18ビットの出力パラメータを有するC A V Eアルゴリズムが、A3アルゴリズムとして使用される。C A V Eアルゴリズムの入力パラメータと、G S M型の入力パラメータ、即ちランダム番号R A N D及び確認キーK iとの間、及びC A V Eアルゴリズムの出力パラメータと、G S Mの出力パラメータ、即ち符号応答S R E Sとの間に、パラメータ適応機能が与えられる。



【特許請求の範囲】

1. 移動通信ネットワークのための確証センターにおいて、

上記移動通信ネットワークの各加入者のための確証キーを記憶するデータベースを備え、上記確証キーは、暗号キー及び確証応答パラメータを計算するための入力パラメータであって、第1の確証手順に必要なフォーマットにあり、

更に、ランダム番号のソースを備え、このランダム番号は、暗号キー及び確証応答パラメータを計算するための別の入力パラメータであって、上記第1の確証手順に必要なフォーマットにあり、

更に、上記データベースからの確証キー及び上記ランダム番号のソースからのランダム番号を入力パラメータとして有し、そして上記第1の確証手順に基づくフォーマットで暗号キーを出力する暗号キー計算ユニットと、

単一入力パラメータを必要とし、そして上記第1の確証手順に基づく確証応答パラメータのフォーマット以外のフォーマットで確証応答パラメータを出力する確証応答パラメータ計算ユニットと、

入力パラメータとしての上記確証キー及び上記ランダム番号にตอบสนองして、上記単一入力パラメータを上記確証応答計算ユニットに与えるための第1の適応ユニットと、

上記確証応答パラメータ計算ユニットにより出力される上記確証応答パラメータにตอบสนองして、上記第1の確証手順に基づく確証応答パラメータを与えるための第2の適応ユニットと、

を備えたことを特徴とする確証センター。

2. 移動ステーションの確証パラメータ処理ユニットにおいて、

上記移動ステーションを使用する移動加入者のための確証キーを記憶するメモリを備え、上記確証キーは、暗号キー及び確証応答パラメータを計算するための入力パラメータであって、第1の確証手順に必要なフォーマットにあり、

更に、ランダム番号のソースを備え、このランダム番号は、暗号キー及び確証応答パラメータを計算するための別の入力パラメータであって、上記第1の確証手順に必要なフォーマットにあり、

更に、上記データベースからの確証キー及び上記ランダム番号のソースから

のランダム番号を入力パラメータとして有し、そして上記第1の確証手順に基づくフォーマットで暗号キーを出力する暗号キー計算ユニットと、

単一入力パラメータを必要とし、そして上記第1の確証手順に基づく確証応答パラメータのフォーマット以外のフォーマットで確証応答パラメータを出力する確証応答パラメータ計算ユニットと、

入力パラメータとしての上記確証キー及び上記ランダム番号に応答して、上記単一入力パラメータを上記確証応答計算ユニットに与えるための第1の適応ユニットと、

上記確証応答パラメータ計算ユニットにより出力される上記確証応答パラメータに応答して、上記第1の確証手順に基づく確証応答パラメータを与えるための第2の適応ユニットと、

を備えたことを特徴とする確証パラメータ処理ユニット。

3. 第1の確証応答計算方法と共に使用されるよう意図された確証手順を使用し；

上記第1の確証応答計算方法に代わって第2の確証応答計算方法を使用し；

上記第1の確証応答計算方法には適合するが上記第2の確証応答計算方法には適合しない確証キーを上記移動通信ネットワークの各加入者ごとに与え；

上記第1の確証応答計算方法には適合するが上記第2の確証応答計算方法には適合しないランダム番号を発生し；

上記確証キー及び上記ランダム番号から上記第2の確証応答計算方法に適合する入力パラメータを導出し；

上記移動通信ネットワークに使用される上記確証手順の確証応答フォーマットに適合しない確証応答を上記第2の確証応答計算方法により計算し；

この確証応答を上記確証手順の確証応答フォーマットに適合するフォーマットに変更し；そして

上記確証応答を上記確証手順に適合する上記フォーマットで移動通信ネットワークにおいて転送して記憶する；

という段階を備えたことを特徴とする移動通信ネットワークのための確証方法。

4. GSMをベースとする確証応答計算方法と共に使用されるよう意図されたGSMをベースとする確証手順を使用し、上記GSMをベースとする確証応答

計算方法は、128ビットのランダム番号RAND及びNビットの確証キーKiを入力パラメータとして含むと共に、32ビットの符号応答SRESを出力パラメータとして含み、Nは、正の整数であり；

上記GSMをベースとする確証応答計算方法に代わる確証応答計算方法としてCAVE計算方法を使用し、このCAVE方法は、152ビットの入力パラメータ及び18ビットの出力パラメータを含み；

移動通信ネットワークの各加入者に対して上記NビットのKiの独特の値を与え；

Kiの上記値を確証センターのデータベースに記憶し；

上記移動加入者の1人に対し上記SRESを与えるための要求を受け取り；

上記移動加入者の上記1人の上記NビットのKiを上記データベースから検索し；

上記128ビットのRANDを発生し；

上記NビットのKi及び128ビットのRANDから上記152ビットの入力パラメータを導出し；

上記CAVE計算方法により上記18ビット出力パラメータを計算し；

上記18ビット出力パラメータに付加的な14ビットをパッドして、上記32ビットのSRESを得；そして

上記GSMをベースとする確証手順に基づき上記GSMをベースとする移動通信ネットワークにおいて上記32ビットSRESを転送しそして記憶する；

という段階を備えたことを特徴とするGSMをベースとする移動通信ネットワークのための確証方法。

5. 上記導出段階は、

上記128ビットのRANDを(152-N)ビットの裁断されたRANDへと裁断し、Nは、128以下の整数であり、そして

上記(152-N)ビットの裁断されたRANDを上記NビットのKiと合

成して、上記152ビットの入力パラメータを得る、

という段階を含む請求項4に記載の方法。

6. GSMをベースとする確証応答計算方法と共に使用されるよう意図された

GSMをベースとする確証手順を使用し、上記GSMをベースとする確証応答計算方法は、128ビットのランダム番号RAND及びNビットの確証キーKiを入力パラメータとして含むと共に、32ビットの符号応答SRESを出力パラメータとして含み、Nは、正の整数であり；

上記GSMをベースとする確証応答計算方法に代わる確証応答計算方法としてCAVE計算方法を使用し、このCAVE方法は、152ビットの入力パラメータ及び18ビットの出力パラメータを含み；

移動加入者に対して与えられた上記NビットのKiの独特の値を移動ステーションのメモリに記憶し；

上記128ビットのRANDを含む確証要求を上記移動ステーションによりベースステーションから受け取り；

上記NビットのKiを上記メモリから検索し；

上記NビットのKi及び128ビットのRANDから上記152ビットの入力パラメータを導出し；

上記CAVE計算方法により上記18ビット出力パラメータを計算し；

上記18ビット出力パラメータに付加的な14ビットをパッドして、上記32ビットのSRESを得；そして

上記32ビットSRESを上記ベースステーションへ送信する；

という段階を備えたことを特徴とするGSMをベースとする移動通信ネットワークのための確証方法。

7. 上記導出段階は、

上記128ビットのRANDを $(152 - N)$ ビットの裁断されたRANDへと裁断し、Nは、128以下の整数であり、そして

上記 $(152 - N)$ ビットの裁断されたRANDを上記NビットのKiと合成して、上記152ビットの入力パラメータを得る、

という段階を含む請求項6に記載の方法。

8. 移動通信システムのための確証パラメータ計算ユニットにおいて、

152ビットの入力パラメータを受け取る第1入力と、18ビットの出力パラメータを出力する出力とを有するCAVEアルゴリズム計算器と、

128ビットのランダム番号RANDを受け取る第1入力と、正の整数をNとすれば、Nビットの確証キーKiを受け取る第2入力と、このNビットのKi及び128ビットのRANDから導出された上記152ビットの入力パラメータを上記CAVEアルゴリズム計算器の上記入力へ出力するための出力とを有する第1アダプタと、

上記CAVEアルゴリズム計算器の18ビット出力パラメータを受け取る入力と、32ビットの符号応答SRESを出力する出力とを有する第2アダプタとを備え、上記Ki、RAND及びSRESは、GSMベースの確証パラメータであることを特徴とする確証パラメータ計算ユニット。

【発明の詳細な説明】

移動通信システムにおける加入者確証

発明の分野

本発明は、移動通信ネットワークのセキュリティ機能に係り、より詳細には、移動通信ネットワークにおいて加入者の確証を得ることに係る。

先行技術の説明

全てのテレコミュニケーションネットワークにおいて、ユーザ及びネットワークオペレータの両方を第三者の不所望な侵入に対してできるだけ保護しなければならない。従って、ネットワークには、多数の種類のセキュリティ機能が必要となる。ネットワークセキュリティの重要な観点は、1) ネットワークが搬送する情報の保護と、2) ネットワークのユーザの確証及びアクセス制御である。情報を保護するためのほとんどのセキュリティ機構は、ある形態の暗号化であり、それに留まり勝ちである。確証は、送って来るように請求されたソースから情報が確実に送られるように試みる手段である。これは、一般に、パスワード及びキーに基づいている。アクセス権は、送信媒体を経て送信及び／又は受信する能力に関して指定される。又、アクセス機構も、一般に、ある形態のパスワード又はキーに基づいている。

移動加入者への送信に無線通信が使用されるために、公衆地上移動ネットワーク(PLMN)のような無線アクセスネットワークは、特に、許可のないユーザによるリソースの誤用や、無線経路上で交換される情報の盗み聞きを感知する。これは、ユーザ又はオペレータの装置を変造せずに、どこからでも無線信号を聞いたり送信したりできることによるものである。PLMNは、通常のテレコミュニケーションネットワークよりも高いレベルのセキュリティを必要とすることが明らかである。

GSM(移動通信用のグローバルシステム)として知られているパン・ヨーロッパアンデジタルセルラー無線は、機密性の高い確証システムを含んでいる。これは、いわゆるチャレンジ・アンド・レスポンスの原理に基づくものである。加入時に、加入者確証キー(Ki)と称する機密番号が、国際移動加入者認識(IMSI)と共に加入者に割り当てられる。この加入者確証キーKiは、加入

者のホーム位置レジスタ（HLR）に関連するか又はそれにリンクされた確証センター（AUC）と称するGSMネットワークの特殊目的の要素に記憶される。AUCは、A8と称する暗号化アルゴリズムと、A3と称する確証アルゴリズムと、ランダム番号RANDの発生機能も備えている。暗号キーKcと称するパラメータがアルゴリズムA8によりKi及びRANDから発生される。同様に、符号応答SRESと称するパラメータが、アルゴリズムA3によりKi及びRANDから発生される。3つのパラメータRAND、Kc及びSRESは、更なる確証及び暗号化に使用されるべき加入者特有の「トリプレット（3つ組）」を形成する。必要になるたびにトリプレットが計算されて転送されるのを回避するために、AUC／HLRにより各加入者ごとに前もって多数のトリプレットが計算され、そして要求時応じて、ビジター位置レジスタ（VLR）及び移動サービス交換センター（MSC）へ送られて、そこに記憶される。MSC／VLRは、そのビジター加入者の各々に対して少なくとも1つの未使用のトリプレットを常に有する。厳密なセキュリティは、1つの通信に対してトリプレットが1回だけ使用され、そして破壊されることを要求する。加入者がその全ての使用可能なトリプレットを使用すると、AUC／HLRは、新たな一連のトリプレットを計算して返送することが要求される。

GSM移動ステーションは、2つの部分に分割され、その一方の部分は、無線インターフェイス及び移動装置に特有のハードウェア及びソフトウェアを含み、そして別の部分は、加入者特有のデータ、即ち加入者認識モジュール即ちSIMを含む。各加入者は、通常は、スマートカードの形態でSIMを有し、これは、移動ステーション側のほとんどのセキュリティ機能に対し責任を負う。これは、Ki、確証アルゴリズムA3、暗号化アルゴリズムA8、及びネットワーク側から受け取った暗号化キーKcを記憶する。

確証の間に、VLR／MSCは、トリプレットのランダム番号RAND（及びKcも）を移動ステーションに送信する。移動ステーション、特に、SIMは、確証アルゴリズムA3及び確証キーKiを用いてRANDを処理し、そしてそれにより得られる符号応答SRESをVLR／MSCに返送する。このSRESはHLRにより与えられたトリプレットのSRESに対してチェックされる。2つ

のSRESが互いに等しい場合には、アクセスが許され、さもなくば、拒絶される。

GSMの全てのセキュリティ機構は、確証キー K_i の機密性に依存する。 K_i は決して送信されず且つAUC/HLRから決して出ない。又、SIMは、 K_i を読み取りに対して完全に保護する。数学的アルゴリズムA3は、一方向にしか働かない（一方向トラップドア機能）ので、送信されたRAND-SRES対からキー K_i を導出することは不可能である。更に、確証アルゴリズムA3自体は機密のアルゴリズムであり、GSM仕様において見つけることができない。この仕様は、RAND及びSRESを知った上での K_i の計算をできるだけ複雑にしなければならないことを要求するだけである。このレベルの複雑さは、どのセキュリティレベルが達成されたかを決定する。この要求を越えてA3に課せられる唯一の制約は、入力パラメータのサイズ（RANDは長さが128ビット）及び出力パラメータのサイズ（SRESは長さが32ビットなければならない）である。 K_i は、AUC/HLRに記憶されるときはいかなるフォーマット及び長さでもよいが、 K_i がネットワークにおいて搬送される場合だけは、128ビットの最大長さに制約される。実際に、移動ステーション及びインフラストラクチャーの両方におけるGSMの設計選択は、オペレータが、他のオペレータとは独立してそれ自身の加入者に適用できるA3を選択できるようにする。

米国内では、パーソナルコミュニケーションシステム（PCS）と称するデジタルセルラーシステムが開発中である。このUS PCSは、特に、セキュリティ機能を含むネットワークアーキテクチャー及びプロトコルに関してGSMシステムに著しく依存している。しかしながら、システムの種々の部分において幾つかの僅かな変更がなされる。1つの潜在的な変更は、GSMシステムに使用される確証アルゴリズムA3がUS PCSのCAVEアルゴリズムに置き換えられることである。というのは、CAVEアルゴリズムは、米国内で開発されたものであり、アナログAMPS（アドバンスト・モバイル・ホーン・サービス）ネットワークに既に使用されているからである。PCSシステムにおいて確証のために使用するのに適したCAVEアルゴリズムは、多数の連結情報フィールドより成る152ビットの入力パラメータと、18ビットの出力パラメータとを有し、

これに対して、GSMのA3アルゴリズムは、128ビットのKi及びRANDパラメータを入力パラメータとして有しそして32ビットのSRESパラメータを出力パラメータとして有する。それ故、GSMベースの移動通信システムにおいてA3をCAVEアルゴリズムに置き換えることは、更なる変更なしに行うことができない。しかしながら、これらの変更は、システム全体にわたって種々のプロトコル、機能、メッセージ及びデータ構造に明らかに影響を及ぼし、CAVEアルゴリズムが技術的にも経済的にも魅力的ではなくなる。更に別の欠点は、GSMシステムとの互換性が失われ、従って、例えば、SIMがGSMシステムとUSPCSシステムとの間をローミングすることができなくなる。

発明の要旨

本発明の目的は、GSMシステム又はGSMをベースとする移動通信ネットワークにおいてGSMの確証パラメータの変更を招くことなくCAVEアルゴリズムをA3アルゴリズムとして使用できるようにすることである。

本発明の別の目的は、GSMシステム又はGSMをベースとする移動通信ネットワークにおいてGSMのトリプレットデータ構造を変更することなくCAVEアルゴリズムをA3アルゴリズムとして使用できるようにすることである。

本発明の更に別の目的は、GSMシステム又はGSMをベースとする移動通信ネットワークにおいて標準的なGSMシステムのセキュリティ機能を保持しながらCAVEアルゴリズムをA3アルゴリズムとして使用できるようにすることである。

本発明の1つの特徴は、第1の確証応答計算方法と共に使用されるよう意図された確証手順を使用し；上記第1の確証応答計算方法に代わって第2の確証応答計算方法を使用し；上記第1の確証応答計算方法には適合するが上記第2の確証応答計算方法には適合しない確証キーを上記移動通信ネットワークの各加入者ごとに与え；上記第1の確証応答計算方法には適合するが上記第2の確証応答計算方法には適合しないランダム番号を発生し；上記確証キー及び上記ランダム番号から上記第2の確証応答計算方法に適合する入力パラメータを導出し；上記移動通信ネットワークに使用される上記確証手順の確証応答フォーマットに適合しない確証応答を上記第2の確証応答計算方法により計算し；この確証応答を上記確

証手順の確証応答フォーマットに適合するフォーマットに変更し；そして上記確証応答を上記確証手順に適合する上記フォーマットで移動通信ネットワークにおいて転送して記憶する、という段階を備えた移動通信ネットワークのための確証方法に係る。

本発明によれば、CAVEアルゴリズムの入力パラメータと、GSM型の入力パラメータ、即ちランダム番号RAND及び確証キーKiとの間、及びCAVEアルゴリズムの出力パラメータと、GSMの出力パラメータ、即ち符号応答SRESとの間に、パラメータ適応機能が与えられる。その結果、CAVEアルゴリズム自体に変更は必要とされず、又、確証センターのAUC/HLR及び移動ステーションMSにおいてSRESを計算する以外、GSM型のセキュリティ機能から何ら逸脱する必要もない。

図面の簡単な説明

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

図1は、GSMをベースとするセルラー移動無線システムを示すブロック図である。

図2は、確証センターAUCにおける公知の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図3は、移動ステーションMSにおける公知の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図4は、MSC/VLRにおける確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図5は、確証及び暗号化パラメータの発生、転送及び使用に関連した信号を示す図である。

図6は、確証センターAUCにおける本発明の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図7は、移動ステーションMSにおける本発明の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

好ましい実施形態の詳細な説明

本発明は、パン・ヨーロッパデジタル移動無線システムGSM又はGSMをベースとする移動無線システム、例えば、DCS1800デジタル通信システム及び米国のパーソナル・コミュニケーション・システム（PCS）と称するデジタルセルラーシステムに適用することができる。本発明の好ましい実施形態は、標準のGSMシステムに適用するものとして以下に説明するが、その主たる適用分野は、米国のPCSシステムであることが明らかである。GSMシステムの構造及び動作は、当業者に良く知られており、ヨーロッパ・テレコミュニケーションズ・スタンダーズ・インスティテュートETSIで発行されたGSM仕様書に定義されている。移動通信のためのGSMシステム、M. モーリ及びM. ポーテット、パライゼウ、フランス、1992年；ISBN2-9507190-0-7も参照されたい。

GSMシステムの基本的構造が図1に示されている。

GSM構造体は、2つの部分、即ちベースステーションシステム（BSS）とネットワークサブシステム（NSS）とで構成される。BSS及び移動ステーションMSは、無線接続を経て通信する。BSSにおいて、各セルは、ベーストランシーバステーション（BTS）によりサービスされる。BTSのグループは、ベースステーションコントローラ（BSC）に接続され、その機能は、BTSにより使用される無線周波数及びチャンネルを管理することである。BSCは、移動サービス交換センター（MSC）に接続される。MSCは、少なくとも1つの移動ステーションMSを含むコールを交換するためのものである。幾つかのMSCが、公衆交換電話ネットワーク（PSTN）のような他のテレコミュニケーションネットワークに接続され、これらネットワークとコールをやり取りするためのゲートウェイ機能を含む。これらMSCは、ゲートウェイMSC（GMSC）として知られている。

コールのルート指定に関連したデータベースには、2つの主たる形式がある。ホーム位置レジスタ（HLR）は、ネットワークの全ての加入者に関する加入者データを永久的又は半永久的に記憶し、このデータは、加入者がアクセスできるサービスや、加入者の現在位置に関する情報を含む。第2の形式のレジスタは、

ビジター位置レジスタ（VLR）である。VLRは、一般には、1つのMSCに取り付けられるが、多数のMSCにサービスすることもできる。この統合されるネットワーク要素は、ビジターMSC（VMSC）として知られている。移動ステーションMSがアクティブ（登録されて、コールを発したり受けたりできる）であるときには、HLRに保持された移動ステーションMSに関する移動加入者データのほとんどが、移動MSが存在するエリアのMSCのVLRへダウンロード（コピー）される。

上記したように、移動無線サービスにおいては、第三者による不許可のコールの試みや、侵入又は傍聴を防止するように多大な注意を払わねばならない。GSMシステムの保護機構は、発呼又は被呼移動ステーションの確証を得、そして暗号化キーを用いて、トラフィックチャンネルのスピーチ及びデータをエンコードする。

確証及び暗号化キーを与えるためのGSM仕様に基づく公知の機能を、図2、3、4及び5を参照して以下に説明する。

加入時に、加入者確証キー（Ki）と称する機密番号が、国際移動加入者認識（IMSI）と共に移動加入者に割り当てられる。図2に示すように、確証センターAUCは、GSMネットワークの各移動加入者に対する確証キーKiを記憶するデータベース20を備えている。移動加入者のKiは、移動加入者のIMSIをインデックスとして使用してデータベース20から検索することができる。AUCには、更に、暗号化アルゴリズムA8、確証アルゴリズムA3及びランダム番号ジェネレータ21が設けられている。ランダム番号ジェネレータ21は、長さが128バイトのランダム番号RANDを与える。データベース20から検索されたキーKi及びランダム番号ジェネレータ21からのランダム番号RANDは、確証アルゴリズムA3において入力パラメータとして使用され、符号応答SRESを計算すると共に、暗号化アルゴリズムA8において入力パラメータとして使用されて、トラフィックチャンネルエンコードのための暗号化キーKcを計算する。3つのパラメータRAND、SRES及びKcは、移動加入者のためのトリプレット（3つ組）を形成する。

トリプレットは、更に、以下に詳細に述べるように、確証及び暗号化に使用す

るために訪問先のMSC/VLRへ転送される。

トリプレットは、1つの通信に対して1回だけ使用されて、破壊される。必要とされるたびにトリプレットを計算して転送するのを回避するために、AUC/HLRにより各移動加入者ごとに多数のトリプレットが前もって計算され、そして要求に応じて訪問先のMSC/VLRへ供給され、そこに記憶される。

訪問先のMSC/VLRは、加入者ごとに幾つかのこのようなトリプレットの保存情報を、必要に応じて検索するために記憶する。図4には、訪問先のMSC/VLRに維持されたセキュリティパラメータファイル40が例示されている。このファイル40は、各IMSI（加入者）ごとにn個のトリプレット1・・・nを含む。

セキュリティパラメータファイル40のこの保存情報は、移動加入者が最初に訪問先のMSC/VLRに登録されるときに最初に確立され、即ちこれは、HLRから「加入者データ挿入」メッセージにおいてダウンロードされる加入者データの一部分である。加入者が、使用可能な全てのトリプレットを使用してしまうと、AUC/HLRは、新たな一連のトリプレットを計算して返送するよう要求される。図5を参照すれば、このトリプレット補充手順は、「パラメータ送信」メッセージと、その返答である「パラメータ送信結果」メッセージの2つのメッセージで構成される。前者のメッセージは、図2について述べたように、トリプレットを計算するためにKiを検索するのに使用される移動加入者のIMSIを含む。計算されたトリプレットは、「パラメータ送信結果」メッセージMSC/VLRへ送られ、そしてVLRに記憶される。

更に、図4を参照すれば、移動ステーションMSは、アクセス要求をMSC/VLRへ送信する。MSC/VLRは、IMSIをインデックスとして使用してセキュリティパラメータファイルに移動ステーションMSの加入者に対して保存されたトリプレットの1つを検索する。MSC/VLRは、一方では、トラフィックチャンネルの暗号化に使用されるべきKcの値をBSCのチャンネル装置へ搬送し、そして他方では、図4にブロック41で示したように、RANDの値を「確証要求」メッセージにおいてMSへ搬送する。移動ステーションMSは、RANDに基づいて、トリプレットの他の値（SRES及びKc）を計算する。

図3を参照すれば、MSは、移動加入者の暗号キー K_i のコピーと、暗号化アルゴリズムA8と、確証アルゴリズムA3とを記憶する。MSC/VLRのための「確証要求」メッセージを受け取ると、MSは、このメッセージからRANDを抽出し、そしてこのRAND及び記憶された K_i をアルゴリズムA3及びA8に入力し、各々符号応答SRES及び暗号キー K_c を各々計算する。計算されたSRESは、「確証結果」メッセージにおいてMSC/VLRへ搬送され、図4及び5に示すように確証が完了する。

図4を参照すれば、MSC/VLRは、「確証結果」メッセージからSRESの値を抽出し（ブロック42）、そしてファイル40からSRESの記憶された値を検索する（ブロック43）。次いで、この通信のために、他の処理の前に、MSC/VLRは、AUC/HLRで計算されたSRESが、MSで計算されたSRESと同じであることをチェックすることにより（ブロック44）移動加入者を「確証」する。2つの値が同一の場合には、アクセスが許可される（ブロック45）。2つの値が同一でない場合には、アクセスが拒絶される（ブロック46）。

暗号化手順は、本発明には関与せず、ここでは詳細に説明しない。

本発明の先行技術で述べたように、特にセキュリティ機能を含むネットワークアーキテクチャー及びプロトコルに関してGSMシステムに大きく依存するパーソナルコミュニケーションシステム（PCS）と称する米国内のデジタルセルラーシステム又は他のセルラーシステムにおいてはCAVEアルゴリズムを確証アルゴリズムA3として使用する必要がある。CAVEアルゴリズムは、米国内で開発され、CAVEアルゴリズム情報の入手性は、ITAR（米国の国際・トラフィック・アンド・アームズ・レギュレーション）の管理下にある。しかしながら、CAVEは、アナログAMPS（アドバンスト・モバイル・ホーン・サービス）ネットワークに既に使用されており、その入力／出力パラメータは、EIA/TIA規格IS-54に規定されている。CAVEアルゴリズムは、多数の連結情報フィールドより成る152ビットの入力パラメータと、18ビットの出力パラメータとを有する。しかしながら、実際に実施する場合にはGSMシステムのA3アルゴリズムが128ビットの K_i 及びRANDを入力

パラメータとして有しそして32ビットのSRESを出力パラメータとして有するために問題に遭遇する。

これらの問題は、本発明により、CAVEアルゴリズムの入力及び出力においてパラメータの適応を行ったときに克服される。その結果、CAVEアルゴリズム自体に何の変更も必要とされず、又、AUC/HLR及びMSにおいてSRESを計算すること以外、GSM仕様から何ら逸脱する必要もない。

本発明によるパラメータ適応の好ましい実施形態を図6及び7について以下に説明する。

図6を参照すれば、本発明による確証センターAUCは、図2に示されたデータベース20及びジェネレータ21と同様のデータベース60及びランダム番号ジェネレータ61を備えている。データベース60は、IMSIでインデックスされるGSMネットワークの全ての移動加入者に対しGSM仕様に基づいて128ビットの確証キーKiを記憶する。更なる計算のためにKiを選択するところのIMSIは、信号インターフェイス67から受け取られ、この信号インターフェイスは、HLR又はVLRから、例えば、「パラメータ送信」メッセージにおいてそれを受け取る。ランダム番号ジェネレータ61は、128ビットのランダム番号RANDをGSM仕様に基づいて発生する。

Ki及びRANDは、暗号化アルゴリズムA8に入力され、このアルゴリズムは、GSMの仕様に基づいて64ビットの暗号化キーKcを計算する。換言すれば、Kcの計算は、図2を参照して説明したものと同一である。

又、128ビットのRANDは、裁断ユニット62にも入力され、該ユニットは、RANDを24ビットの裁断されたRAND(TRANDED)へと裁断する。TRANDEDは、例えば、RANDの最上位24ビットを含む。しかしながら、ここで使用する裁断動作は、128ビットのランダム番号RANDから24ビットのランダム番号TRANDEDを導出するためのいかなる方法も包含することが明らかである。Kiの長さは、好ましい実施形態では128ビットであるが、128以下の整数をNとすれば、Nビットの長さでよいことに注意されたい。従って、TRANDEDの長さMは、Nに依存し、 $M = 128 - N$ ビットである。

24ビットのTRANDEDは、次いで、合成ユニット63に入力され、該ユニッ

ト63の他方の入力は、128ビットの確証キー K_i である。合成ユニット63の出力は、 K_i 及び $TRAND$ の152ビットの組合せ $COMP$ である。 $COMP$ の最上位128ビットは、 K_i を含み、そして最下位24ビットは、 $TRAND$ を含む。しかしながら、ここで使用する合成動作は、 K_i と $TRAND$ を合成することにより152ビット値を導出するための例えば論理演算のような方法を包含することが明らかである。

152ビットの $COMP$ パラメータは、計算ユニット65において $CAVE$ アルゴリズムの入力パラメータに設定される要件を満足する。従って、本発明によるパラメータ適応は、 GSM 適合の入力パラメータ K_i 及び $RAND$ から $CAVE$ 適合の入力パラメータを導出する。計算の結果として、 $CAVE$ 計算ユニット65は、18ビットの出力パラメータを出力する。

$CAVE$ からの18ビットの出力パラメータは、次いで、パッドユニット64に入力され、ここでは、14のスタフビットが挿入されて、32ビット値が得られる。14のスタフビットは、例えば、32ビットパラメータの最下位14ビットを確立し、最上位18ビットは、 $CAVE$ 65からの18ビット出力を含む。しかしながら、ここで使用するパッド動作は、18ビットの $CAVE$ 出力パラメータを14ビットだけ延長して32ビットを得るための例えば論理演算のような何らかの方法を包含することが明らかであろう。

これにより得られる32ビットの出力パラメータは、次いで、 GSM 仕様に基づく符号応答 $SRES$ として使用される。従って、本発明によるパラメータ適応は、 $CAVE$ 適合出力パラメータから GSM 適合の出力パラメータを導出する。

3つの GSM 適合のセキュリティパラメータ $SRES$ 、 K_c 及び $RAND$ は、標準的な GSM トリプレットを形成するトリプレット形成ユニット66に入力される。トリプレットは、信号インターフェイス67を経て HLR 又は VLR に転送される。従って、 $SRES$ は、標準的な $SRES$ と同様に、 GSM ネットワークにおいて転送されそして処理される。

図7を参照すれば、本発明による移動ステーション MS は、移動加入者の暗号キー K_i のコピーをメモリ75に記憶する。又、 MS は、暗号化アルゴリズムA8を実行する計算ユニット76と、確証のための $CAVE$ アルゴリズムを実行

する計算ユニット77とを備えている。MSC/VLRから「確証要求」メッセージを受け取ると、無線インターフェイスに特有のハードウェア及びソフトウェアを含むMSの移動装置78は、メッセージからRANDを抽出し、そしてRAND及び記憶されたKiをA8計算ユニット76へ入力し、暗号キーKcを計算する。本発明の好ましい実施形態では、78を除く全ての機能ブロックが、MSの加入者認識モジュール即ちSIMに配置されている。

又、128ビットのRANDは、RANDを24ビットのTRANDに裁断する裁断ユニット72にも入力される。裁断ユニット72は、図6に示す裁断ユニット62と同一である。

24ビットのTRANDは、次いで、128ビットのKiと共に、合成ユニット73に入力される。合成ユニット73の出力は、152ビットのCOMPである。合成ユニット73は、図6に示す合成ユニット63と同一である。

152ビットのCOMPは、次いで、CAVE計算ユニット77に入力され、該ユニットは、18ビットの出力パラメータを出力する。

CAVE77からの18ビット出力パラメータは、パッドユニット74に入力され、ここで、14のスタフビットが取り付けられて、32ビット値が与えられる。パッドユニット74は、図6に示すパッドユニット64と同一である。

それにより得られた32ビットの出力パラメータは、次いで、GSM仕様に基づくSRESパラメータとして使用される。SRESは、移動装置78に返送され、そして更に「確証結果」メッセージにおいてMSC/VLRへ送られ、標準的なGSMシステムの場合と同様にMSC/VLRにおいて処理される。

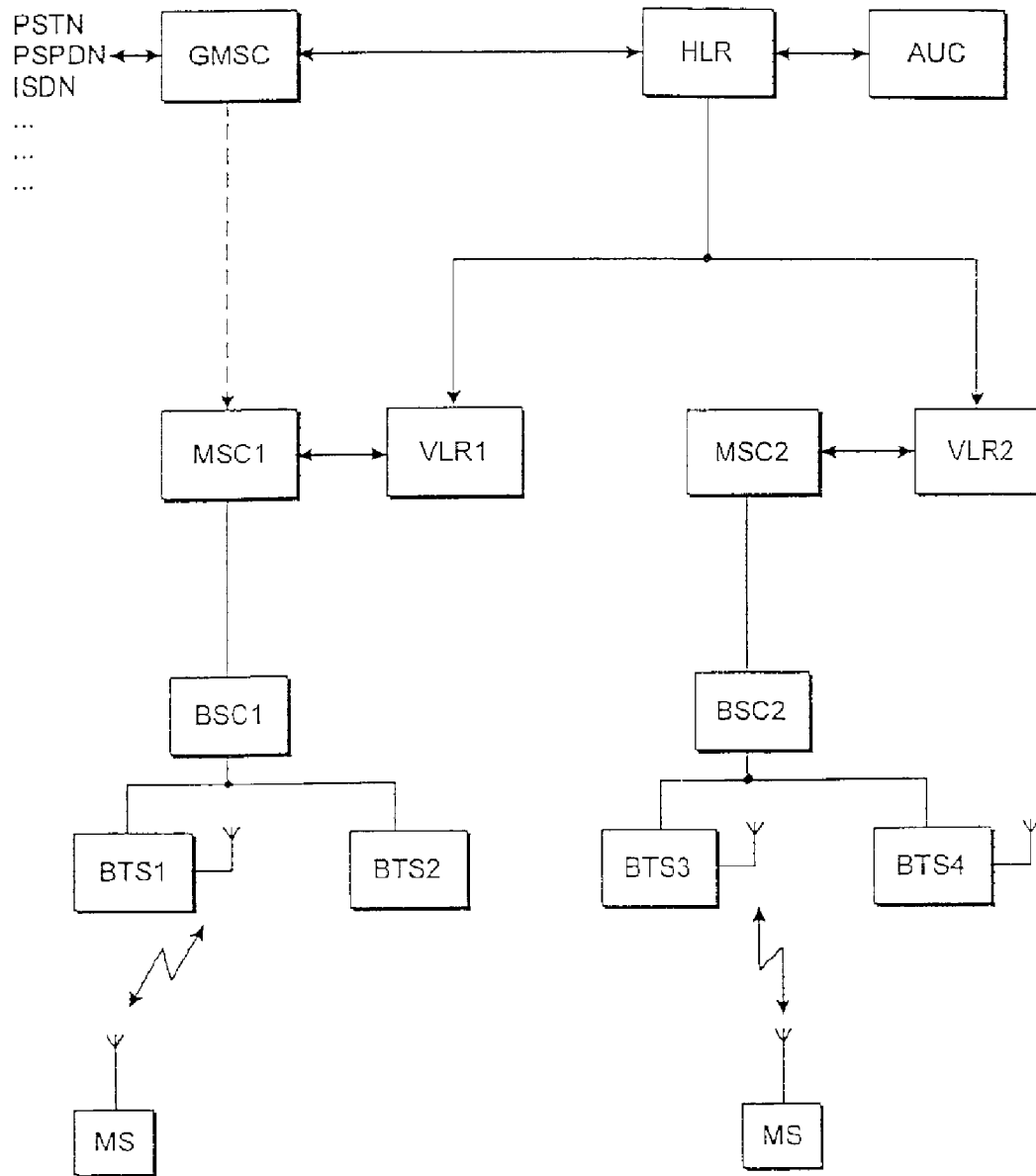
NビットのKi及びRANDパラメータから152ビットのCAVE入力パラメータを導出する別の実施形態が図8に示されている。以下の例では、N=128であるが、これらの実施形態ではいかなる正の整数でもよい。Kiは、2つの部分に分割され、即ちKiの104ビット、例えば、104のLSBビットは、論理ユニット81の入力に送られる。Kiの残りの24ビットは、合成器82に入力される。同様に、RANDも2つの部分に分割され、即ちRANDの104ビット、例えば、104のMSBビットは、論理ユニット81に入力される。RANDの残りの24ビットは、合成器82の別の入力に送られる。2つの

104ビット入力の間でアンド、オア又は排他的オア(XOR)のような論理演算が行われ、単一の104ビット出力が与えられる。論理ユニット81からの104ビット出力は、合成器82に入力される。合成器82は、2つの24ビット入力と104ビット入力を152ビットパラメータへと組み立て、CAVEアルゴリズムへ入力する。図6の確証センター及び図7の移動ステーションに適用されるときは、論理ユニット81及び合成器82が、各々、裁断ユニット62、72及び合成器63、73に置き換えられる。

図8の実施形態に対する更に別の変更として、 K_i の104ビット及びRANDの104ビットが同数のサブブロックに細分化され、異なるサブブロック間で異なる論理演算が実行される。例えば、26ビットの4つのサブブロックが存在する。

添付図面及びそれを参照した以上の説明は、単に本発明を例示するものに過ぎない。請求の範囲から逸脱せずに多数の変更や修正がなされ得ることが当業者に明らかであろう。

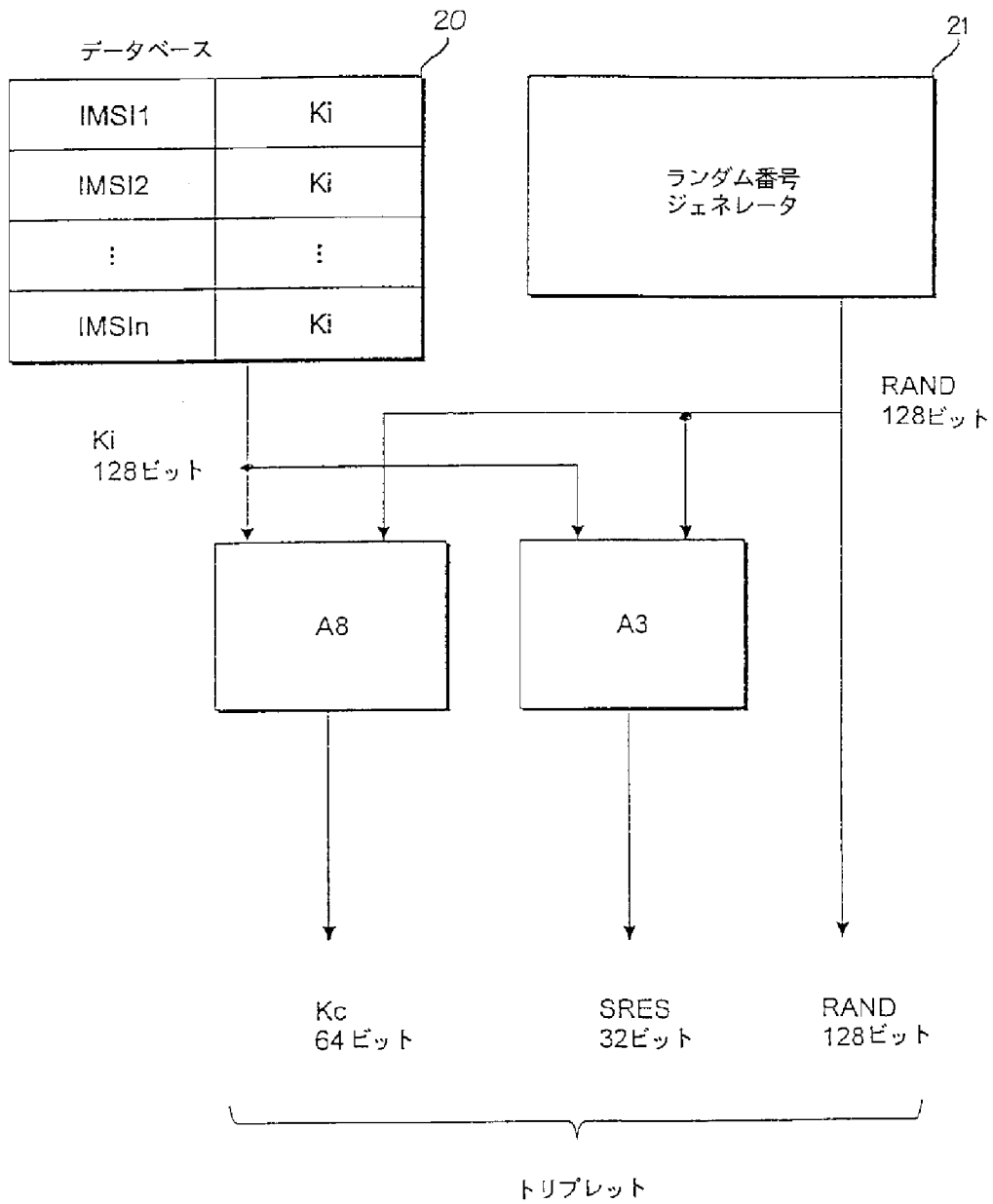
【図1】

Fig. 1
(従来例)

【図2】

Fig. 2

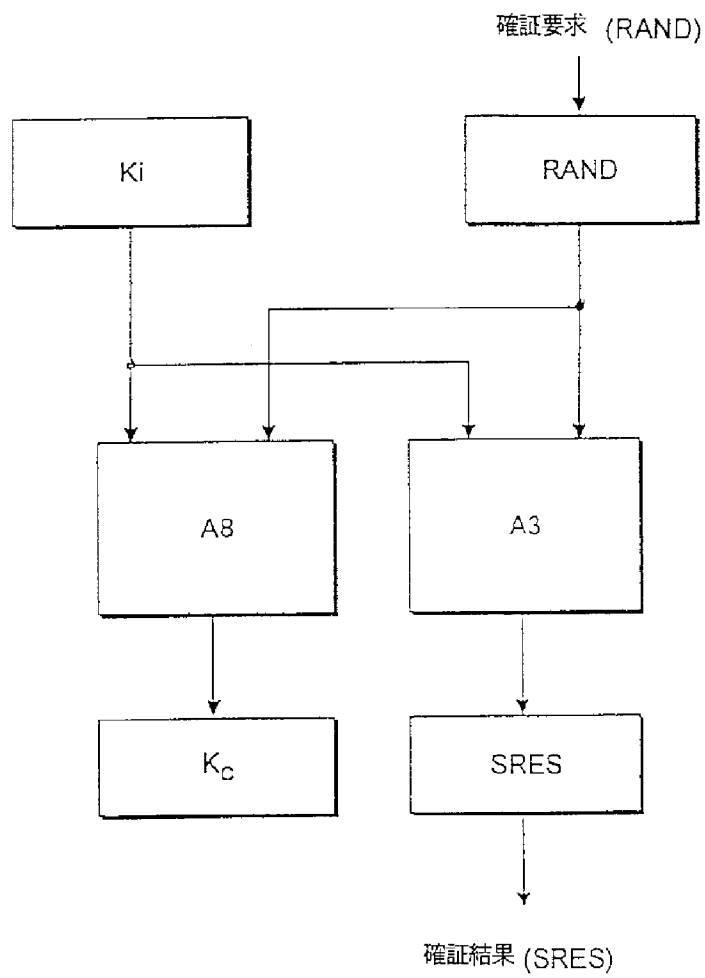
(従来例)



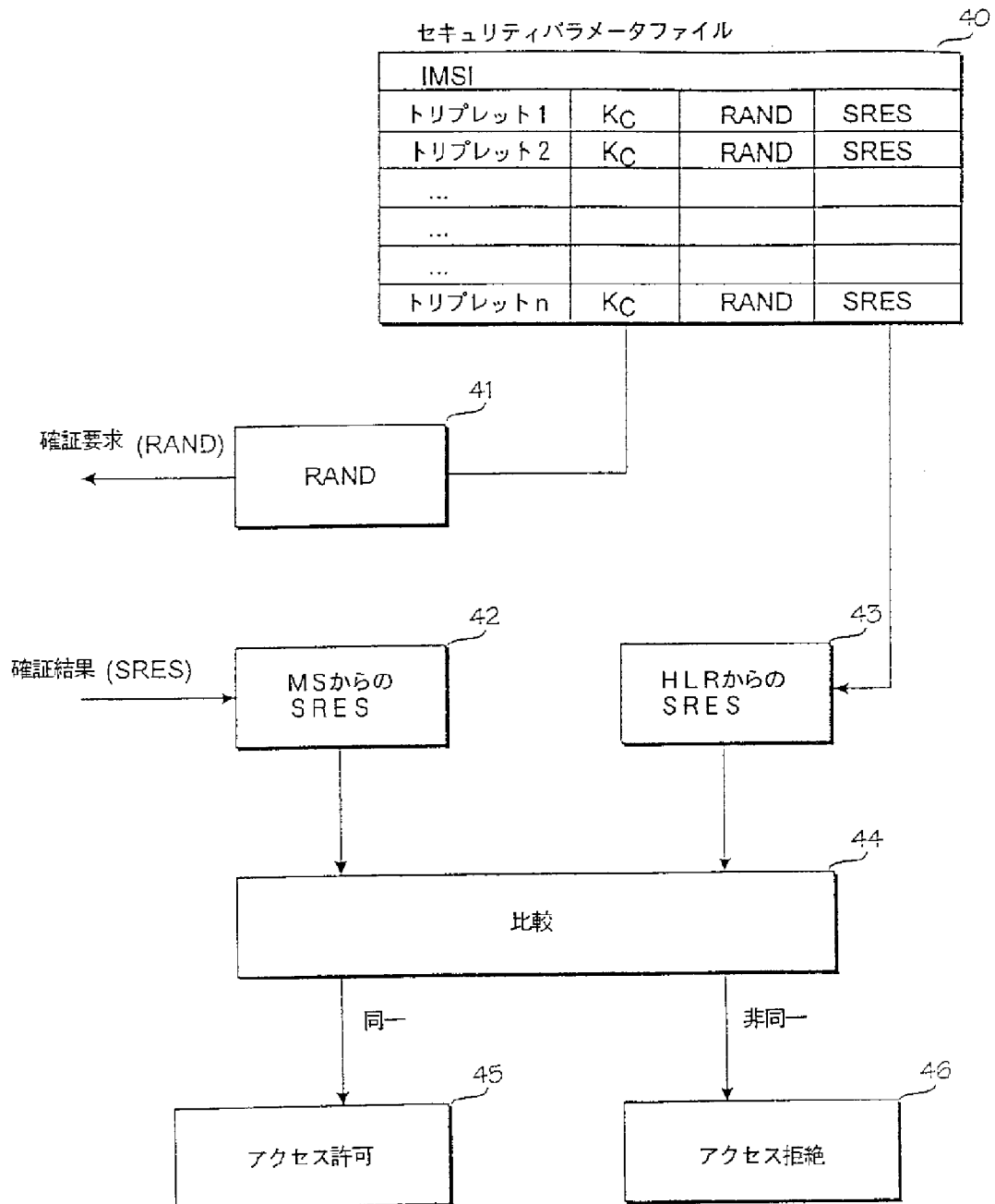
【図3】

Fig. 3

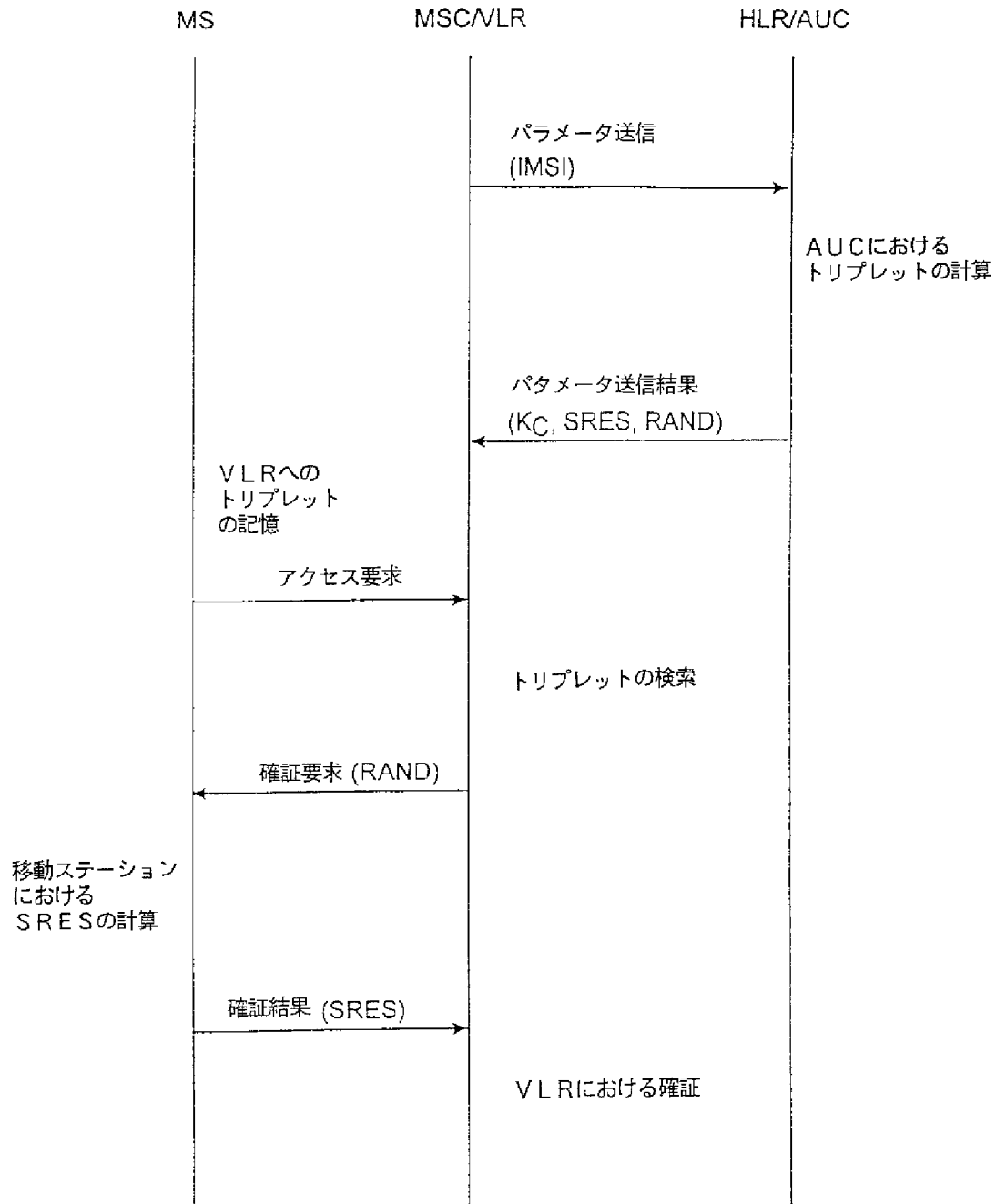
(従来例)



【図4】

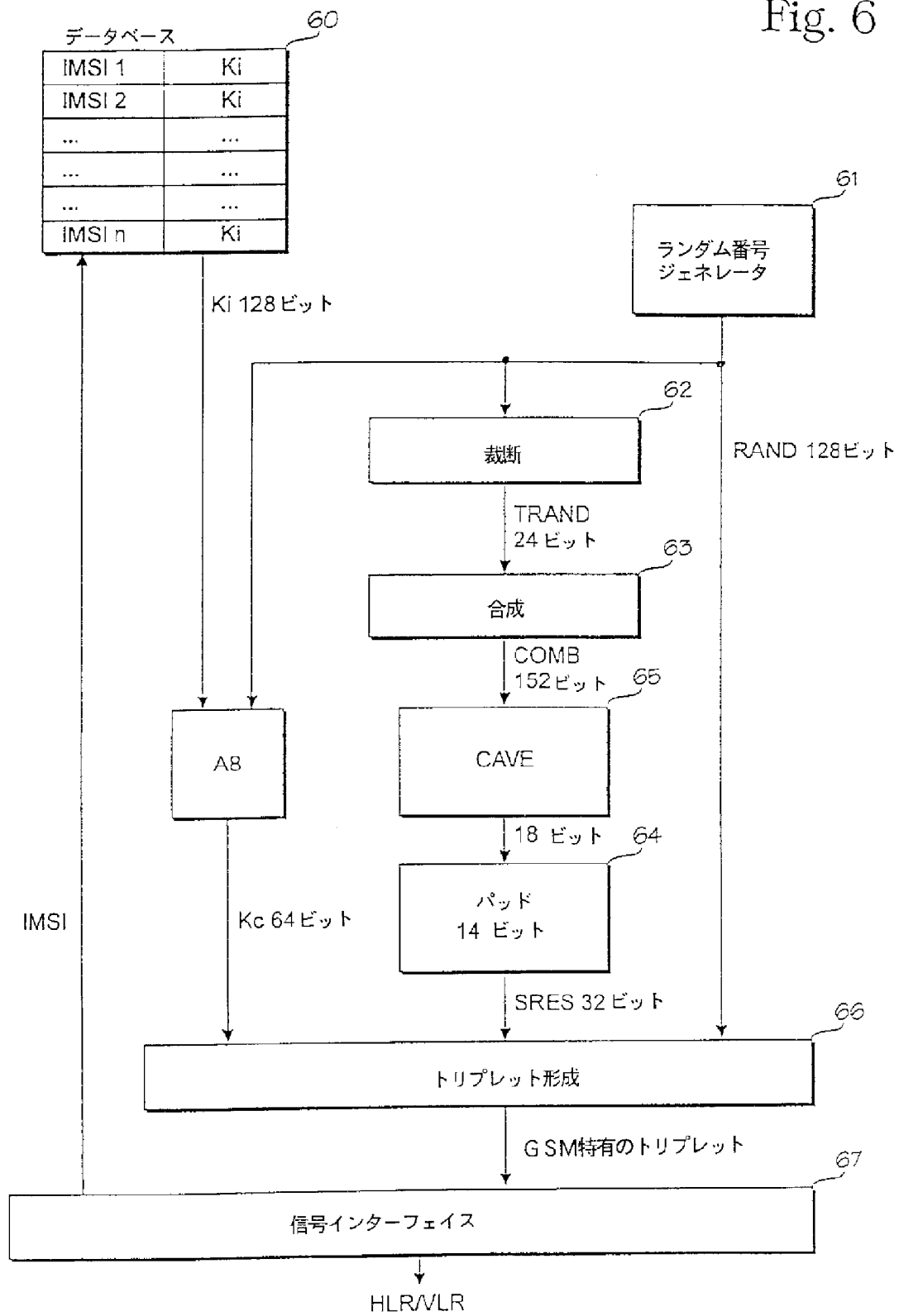
Fig. 4
(従来例)

【図5】

Fig. 5
(従来例)

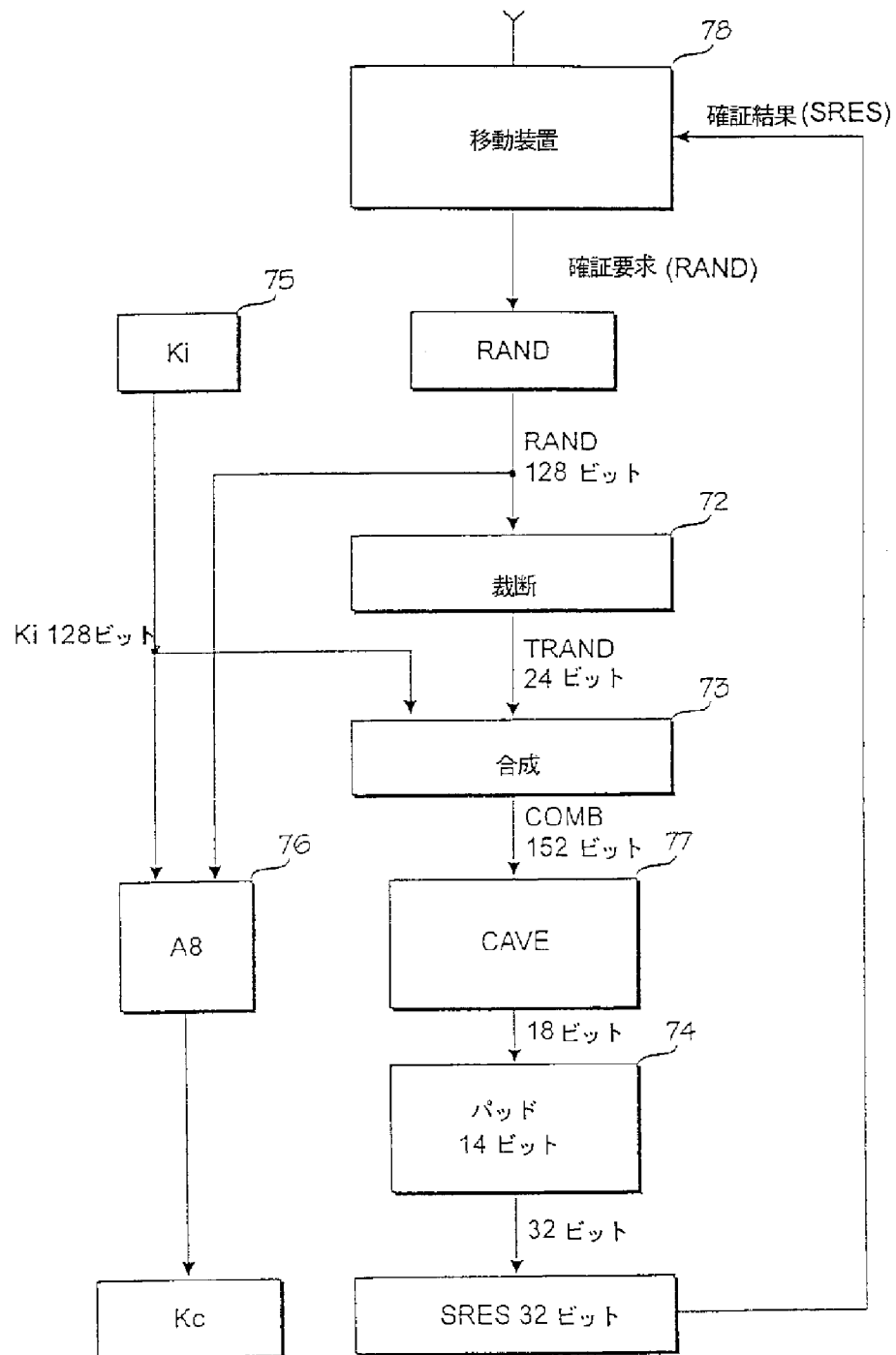
【図6】

Fig. 6



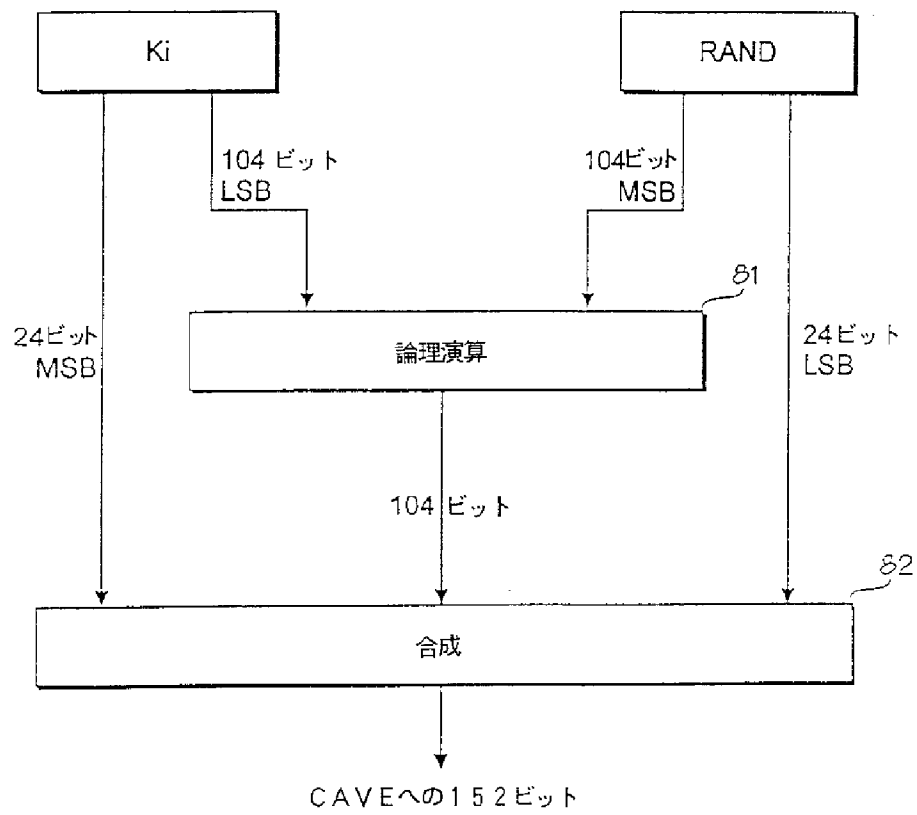
【図7】

Fig. 7



【図8】

Fig. 8



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00543

A. CLASSIFICATION OF SUBJECT MATTER		
IPC6: H04Q 7/38, H04L 9/32 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC6: H04Q, H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
SE,DK,FI,NO classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
INSPEC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0675615 A1 (FRANCE TELECOM), 4 October 1995 (04.10.95), abstract --	1-8
A	US 5319710 A (M. ATALLA ET AL), 7 June 1994 (07.06.94), column 2, line 49 - column 6, line 16 --	1-8
P,A	US 5513245 A (S.MIZIKOVSKY ET AL.), 30 April 1996 (30.04.96), column 3, line 46 - column 4, line 26 -- -----	1-8
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents "A" document defining the general state of the art which is not considered to be of particular relevance "B" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
13 March 1997		20-03-1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86		Authorized officer Christina Halldin Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT
Information on patent family members

03/02/97

International application No.

PCT/FI 96/00543

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0675615	04/10/95	FR-A,B- 2718312 JP-A- 8008899	06/10/95 12/01/96
US-A- 5319710	07/06/94	AU-A- 664823 EP-A- 0678836	07/12/95 25/10/95
US-A- 5513245	30/04/96	NONE	

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN